FIG 1

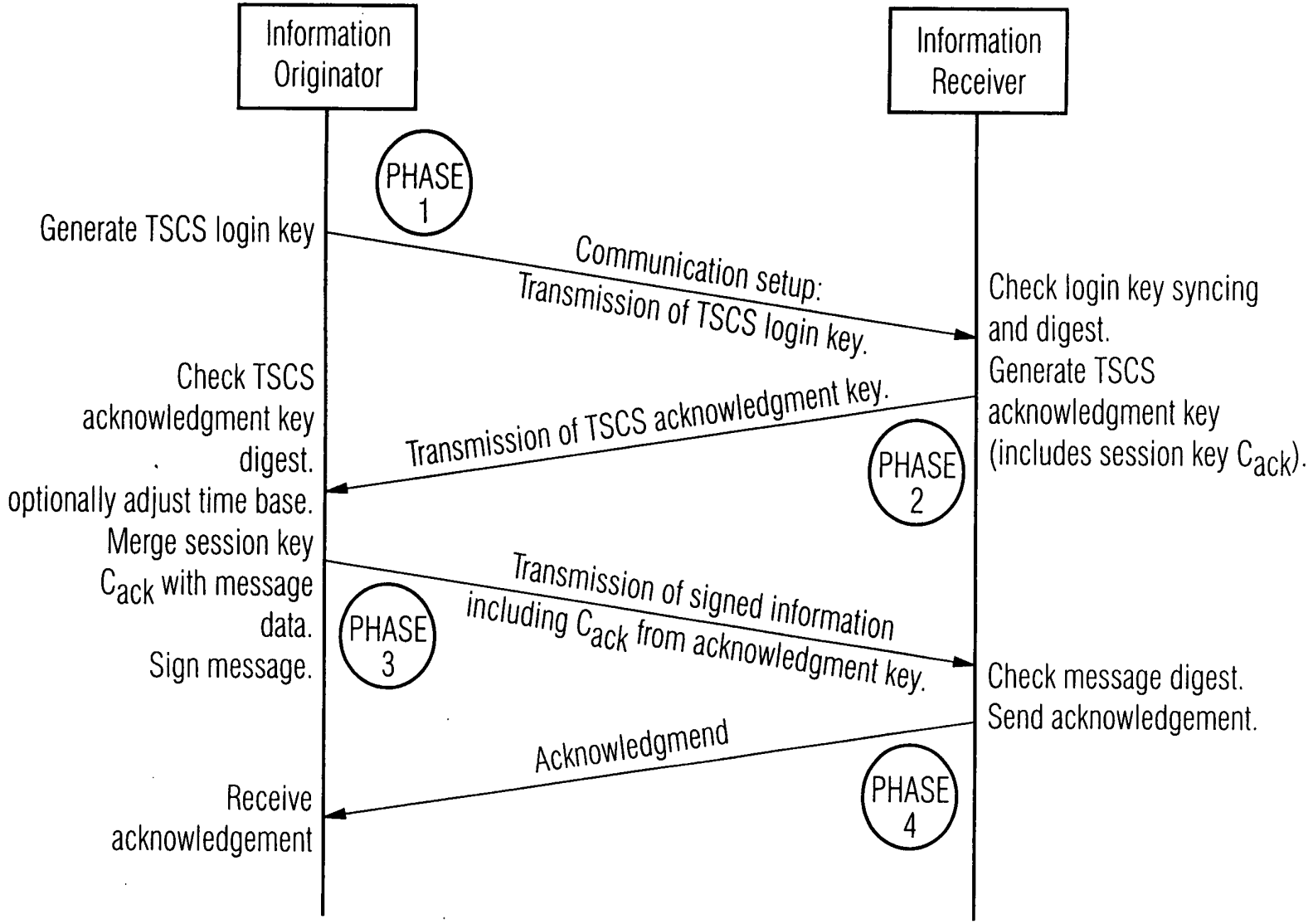

Information Originator
Information Receiver
PHASE 1
Generate TSCS login key
Communication setup:
Transmission of TSCS login key.
Check login key syncing and digest.
Generate TSCS acknowledgment key (includes session key C_{ack}).
Check TSCS acknowledgment key digest.
optionally adjust time base.
Transmission of TSCS acknowledgment key.
PHASE 2
Merge session key C_{ack} with message data.
Sign message.
PHASE 3
Transmission of signed information including C_{ack} from acknowledgment key.
Check message digest.
Send acknowledgement.
Acknowledgmend
Receive acknowledgement
PHASE 4

FIG 2

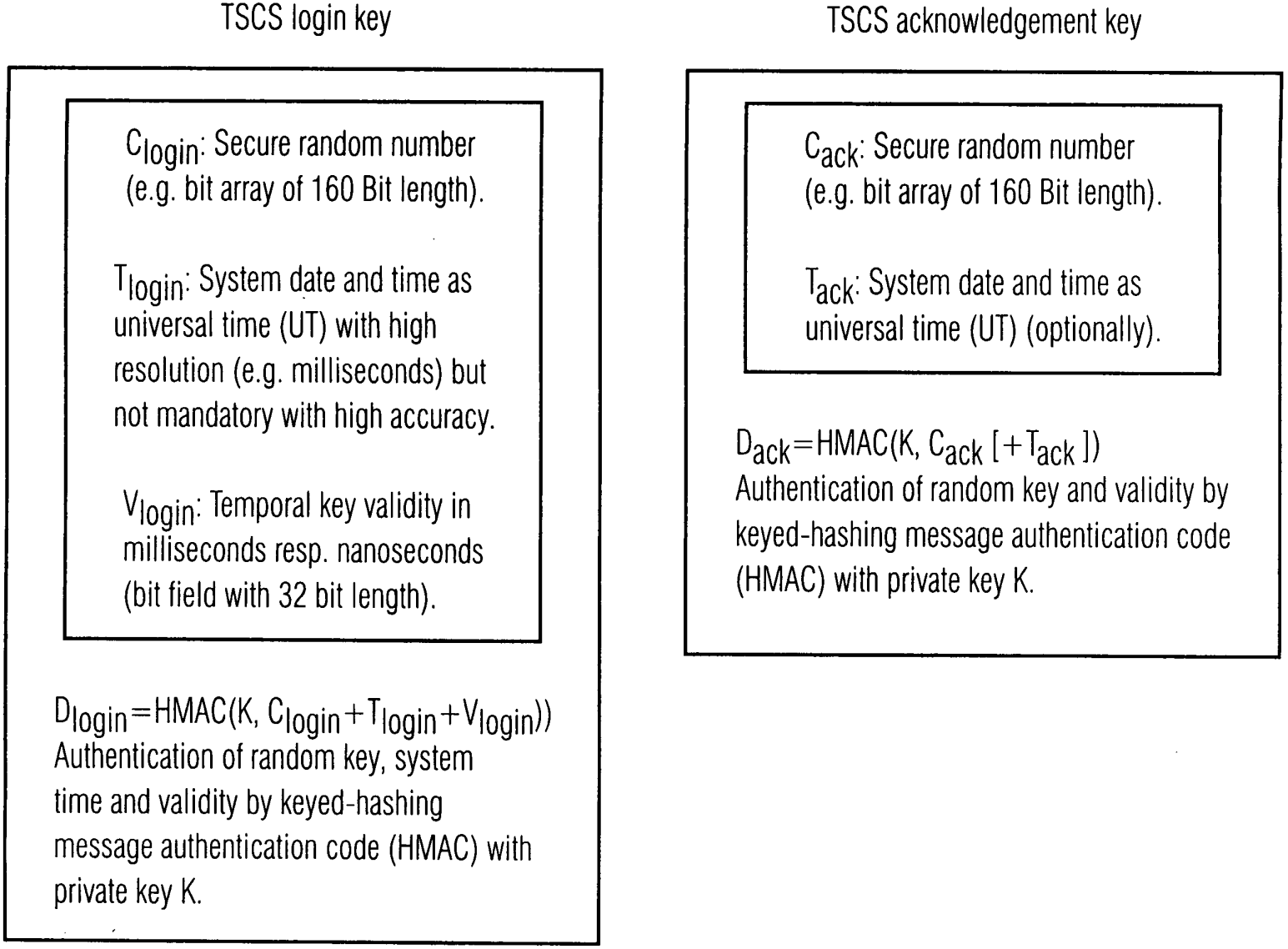
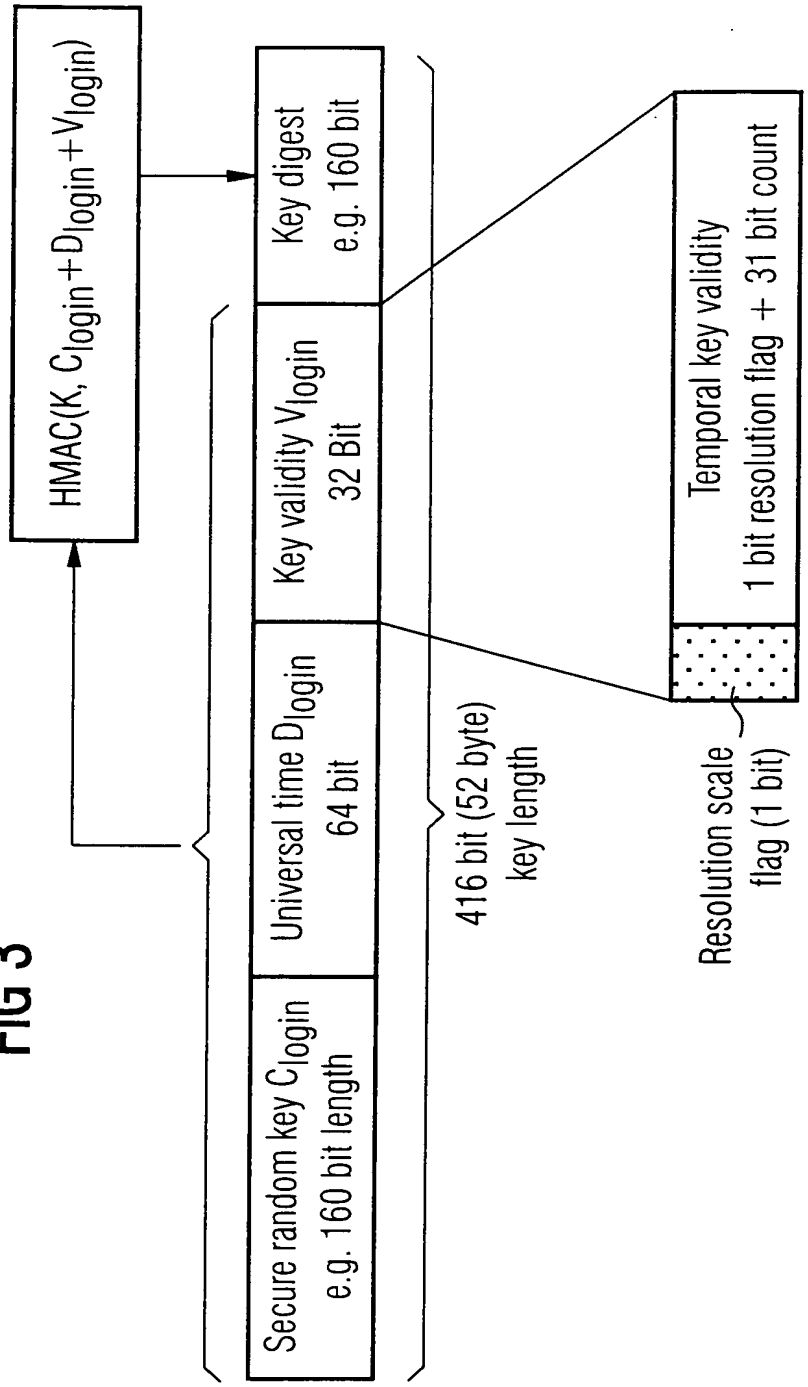

TSCS login key
C_{login}: Secure random number (e.g. bit array of 160 Bit length).
T_{login}: System date and time as universal time (UT) with high resolution (e.g. milliseconds) but not mandatory with high accuracy.
V_{login}: Temporal key validity in milliseconds resp. nanoseconds (bit field with 32 bit length).
$D_{login}=HMAC(K, C_{login}+T_{login}+V_{login})$
Authentication of random key, system time and validity by keyed-hashing message authentication code (HMAC) with private key K.
TSCS acknowledgement key
C_{ack}: Secure random number (e.g. bit array of 160 Bit length).
T_{ack}: System date and time as universal time (UT) (optionally).
$D_{ack}=HMAC(K, C_{ack}[+T_{ack}])$
Authentication of random key and validity by keyed-hashing message authentication code (HMAC) with private key K.

FIG 3


HMAC(K, Clogin+Dlogin+Vlogin)
Secure random key Clogin
e.g. 160 bit length
Universal time Dlogin
64 bit
Key validity Vlogin
32 Bit
Key digest
e.g. 160 bit
416 bit (52 byte)
key length
Resolution scale
flag (1 bit)
Temporal key validity
1 bit resolution flag + 31 bit count